A Note on Projecting the Cubic Lattice

N. J. A. Sloane[(a)], Vinay A. Vaishampayan,
AT&T Shannon Labs,
180 Park Avenue, Florham Park, NJ 07932-0971, USA.
and
Sueli I. R. Costa,
University of Campinas,
Campinas, SP 13083-970, Brazil.

Email: njas@research.att.com, vinay@research.att.com, sueli@ime.unicamp.br.

[(a)] To whom correspondence should be addressed.

April 5, 2010; revised April 24, 2010, May 25 2010, July 14 2010

Abstract

It is shown that, given any $(n-1)$-dimensional lattice Λ, there is a vector $v \in \mathbb{Z}^n$ such that the orthogonal projection of $\mathbb{Z}^n$ onto $v^\perp$ is, up to a similarity, arbitrarily close to Λ. The problem arises in attempting to find the largest cylinder anchored at two points of $\mathbb{Z}^n$ and containing no other points of $\mathbb{Z}^n$.

Keywords: projections, shadows, dense packings
AMS 2010 Classification: Primary 11H55, 52C17

1. Introduction

Let $\mathbb{Z}^n$ denote the cubic lattice with basis $e_1 := (1, 0, \ldots, 0), \ldots, e_n := (0, 0, \ldots, 1)$. If we project $\mathbb{Z}^n$ onto the $(n-1)$-dimensional subspace

$$v^\perp := \{x \in \mathbb{R}^n : x \cdot v = 0\}$$

perpendicular to a vector $v \in \mathbb{Z}^n$, we obtain an $(n-1)$-dimensional lattice that we denote by Λ_v. We will show that, given any $(n-1)$-dimensional lattice Λ, we can choose $v \in \mathbb{Z}^n$ so that Λ_v is arbitrarily close to a lattice that is geometrically similar to Λ. More precisely, we will establish:

Theorem 1. *Let Λ be an $(n-1)$-dimensional lattice with Gram matrix A (with respect to some basis for $\mathbb{R}^{n-1}$). For any $\epsilon > 0$, there exist a nonzero vector $v \in \mathbb{Z}^n$, a basis B for the $(n-1)$-dimensional lattice Λ_v and a number c such that if A_v denotes the Gram matrix of B, then*

$$\|A - cA_v\|_\infty < \epsilon\,. \tag{1}$$

The theorem is at first surprising, since A has $\binom{n+1}{2}$ degrees of freedom, whereas v has only n degrees of freedom (for the explanation see the remark following the proof of Theorem 2).

The problem arises from a question in communication theory (see §5), which calls for projections Λ_v with high packing density. Since both the determinant and minimal norm of a lattice are continuous functions of the entries in the Gram matrix, so is the packing density.[1] The theorem

[1]The minimal norm μ of a d-dimensional lattice with Gram matrix A is the minimum over all $z \in \mathbb{Z}^d$, $z \neq 0$, of the quadratic form zAz^{tr}. It is enough to consider the finite set of z in some ball around the origin. For a given $z \neq 0$, zAz^{tr} is a continuous function of the entries of A, and since the minimum of a finite set of continuous functions is continuous, μ is a continuous function of the entries of A.

therefore implies that the packing density of Λ_v can be made arbitrarily close to that of Λ. So if we know a dense lattice in $\mathbb{R}^{n-1}$, we can find projections that converge to it in density.

Remark. We know (see for example [2, Cor. 8]) that if Λ is a classically integral $(n-1)$-dimensional lattice then Λ can be embedded in some odd unimodular lattice K of dimension $k \le n+2$, although for $n \ge 7$ K need not be $\mathbb{Z}^k$. In any case this does not imply that Λ can be recovered as a projection of K.

Notation. Λ^* denotes the dual lattice to Λ, A^{tr} is the transpose of A, and $\|A\|_\infty = \max_{i,j} |A_{i,j}|$. Our vectors are row vectors. For undefined terms from lattice theory see [3].

2. Proof of Theorem 1

We begin with some preliminary remarks about the projection lattice Λ_v and its dual Λ_v^*. For simplicity we will only consider projections that use vectors of the form $v = (1, v_1, v_2, \ldots, v_{n-1}) \in \mathbb{Z}^n$. Let $\hat{v} := (v_1, v_2, \ldots, v_{n-1})$, $M := \|v\|^2 = 1 + \sum v_i^2$.

The matrix that orthogonally projects $\mathbb{R}^n$ onto $v^\perp$ is $P := I_n - \frac{1}{M} v^{\mathrm{tr}} v$. As a generator matrix G for $\mathbb{Z}^n$ (expressed in terms of $e_1, \ldots, e_n$) we take I_n with its first row replaced by v. Let G_v be obtained by omitting the first (zero) row of GP. Then G_v is an $(n-1) \times n$ generator matrix for the projection lattice Λ_v, and $A_v := G_v G_v^{\mathrm{tr}} = I_{n-1} - \frac{1}{M} \hat{v}^{\mathrm{tr}} \hat{v}$ is its Gram matrix, with $\det \Lambda_v = \det A_v = \frac{1}{M}$.

It is often easier to work with the dual lattice Λ_v^*. This is the intersection of $\mathbb{Z}^n$ with the subspace $v^\perp$, and has generator matrix

$$\begin{bmatrix} -v_1 & 1 & 0 & \ldots & 0 \\ -v_2 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -v_{n-1} & 0 & 0 & \ldots & 1 \end{bmatrix}, \tag{2}$$

Gram matrix $A_v^* = I_{n-1} + \hat{v}^{\mathrm{tr}} \hat{v}$, and determinant M.

If a sequence of matrices T_i converges in the $\| \; \|_\infty$ norm to a positive-definite matrix T, then T_i^{-1} converges to T^{-1}. So the following theorem is equivalent to Theorem 1.

Theorem 2. *Let Λ be an $(n-1)$-dimensional lattice with Gram matrix A (with respect to some basis for $\mathbb{R}^{n-1}$). For any $\epsilon > 0$, there exist a nonzero vector $v \in \mathbb{Z}^n$, a basis B for the $(n-1)$-dimensional lattice Λ_v^* and a number c such that if A_v^* denotes the Gram matrix of B, then*

$$\|A - cA_v^*\|_\infty < \epsilon \,. \tag{3}$$

Proof of Theorem 2. We may write $A = LL^{\mathrm{tr}}$ where $L = [L_{i,j}]$ is an $(n-1) \times (n-1)$ lower triangular matrix. For $w = 1, 2, \ldots$ let us form the $(n-1) \times n$ matrix

$$\begin{aligned} L_w \;&:=\; -\begin{bmatrix} \lfloor wL \rfloor & \mathbf{0} \end{bmatrix} + \begin{bmatrix} \mathbf{0} & I_{n-1} \end{bmatrix} \\ &= \begin{bmatrix} -\lfloor wL_{1,1} \rfloor & 1 & 0 & \ldots & 0 & 0 \\ -\lfloor wL_{2,1} \rfloor & -\lfloor wL_{2,2} \rfloor & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -\lfloor wL_{n-1,1} \rfloor & -\lfloor wL_{n-1,2} \rfloor & -\lfloor wL_{n-1,3} \rfloor & \ldots & -\lfloor wL_{n-1,n-1} \rfloor & 1 \end{bmatrix}, \end{aligned} \tag{4}$$

where $\mathbf{0}$ denotes a column of $n-1$ zeros. We call L_w a "lifted" version of L.

We apply elementary row operations to L_w so as to put it in the form

$$\tilde{L}_w := \begin{bmatrix} -v_1 & 1 & 0 & \dots & 0 & 0 \\ -v_2 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -v_{n-2} & 0 & 0 & \dots & 1 & 0 \\ -v_{n-1} & 0 & 0 & \dots & 0 & 1 \end{bmatrix}, \tag{5}$$

and take $v = (1, v_1, \dots, v_{n-1})$. Then Λ_v^* has generator matrix $\tilde{L}_w$. But $\tilde{L}_w$ and L_w generate the same lattice. It follows that Λ_v^* has a Gram matrix

$$A_v^* = L_w L_w^{\mathrm{tr}} = w^2 A + B = w^2 \big(A + \frac{1}{w^2} B\big), \tag{6}$$

using (4), where the entries in B are of order $O(w)$ as $w \to \infty$. This implies (3) (with $c = 1/w^2$). ■

Remark. The apparent paradox mentioned in §1 is explained by the fact that we use $\binom{n}{2}$ degrees of freedom in going from (4) to (5).

3. Examples

3.1. The lattice $2\mathbb{Z} \oplus \mathbb{Z}$

We start with a concrete example. If we take $v = (1, 1, 0)$ then Λ_v has Gram matrix $\frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$, and is geometrically similar to $\sqrt{2}\mathbb{Z} \oplus \mathbb{Z}$. Similarly $v = (1, 1, 1)$ produces the hexagonal (or A_2) lattice, and in general $v = (1, 1, \dots, 1)$ gives A_{n-1}. On the other hand, there is no $v = (1, v_1, v_2) \in \mathbb{Z}^3$ such that Λ_v is geometrically similar to $2\mathbb{Z} \oplus \mathbb{Z}$ (see Proposition 3). However, we can find projections which converge to a lattice that is geometrically similar to $2\mathbb{Z} \oplus \mathbb{Z}$. Since any two-dimensional lattice is geometrically similar to its dual, we can apply Theorem 2 with $\Lambda = 2\mathbb{Z} \oplus \mathbb{Z}$. Then $L = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$, the lifted generator matrix is $L_w = \begin{bmatrix} -2w & 1 & 0 \\ 0 & -w & 1 \end{bmatrix}$, $\tilde{L}_w = \begin{bmatrix} -2w & 1 & 0 \\ -2w^2 & 0 & 1 \end{bmatrix}$, $v = (1, 2w, 2w^2)$, and a Gram matrix for Λ_v^* is $I_2 + \tilde{v}^{\mathrm{tr}} \tilde{v} = \begin{bmatrix} 4w^2 + 1 & 4w^3 \\ 4w^3 & 4w^4 + 1 \end{bmatrix}$. If we subtract w times the first generator from the second, this becomes

$$\begin{bmatrix} 4w^2 + 1 & -w \\ -w & w^2 + 1 \end{bmatrix} = w^2 \begin{bmatrix} 4 + 1/w^2 & -1/w \\ -1/w & 1 + 1/w^2 \end{bmatrix},$$

which converges to $w^2 \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix}$ as $w \to \infty$.

Proposition 3. *There is no vector $v = (1, a, b) \in \mathbb{Z}^3$ such that Λ_v^* is geometrically similar to $2\mathbb{Z} \oplus \mathbb{Z}$.*

Proof. From (2), Λ_v^* has Gram matrix $A := \begin{bmatrix} a^2+1 & ab \\ ab & b^2+1 \end{bmatrix}$. If Λ_v^* is geometrically similar to $2\mathbb{Z} \oplus \mathbb{Z}$ then there is a matrix $T := \begin{bmatrix} r & s \\ t & u \end{bmatrix} \in SL_2(\mathbb{Z})$ and $\lambda \in \mathbb{R}$ such that

$$A = \lambda T \begin{bmatrix} 4 & 0 \\ 0 & 1 \end{bmatrix} T^{\mathrm{tr}} = \lambda \begin{bmatrix} 4r^2+s^2 & 4rt+su \\ 4rt+su & 4t^2+u^2 \end{bmatrix} .$$

This implies $\lambda \in \mathbb{Q}$, and taking the determinant and trace of both sides we obtain $a^2+b^2+1 = 4\lambda^2$, $a^2+b^2+2 = 4\lambda^2+1 = \lambda\sigma$, where $\sigma := 4r^2+4t^2+s^2+u^2 \in \mathbb{Z}$. Hence the discriminant of the quadratic for λ, $\sigma^2 - 16$, is a perfect square, so $\sigma = 4$ or 5, $\lambda = \frac{1}{2}$, $\frac{1}{4}$ or 1, $a^2+b^2+1 = 1$, $\frac{1}{4}$ or 3, none of which are possible. ■

3.2. The lattice 5_1

For an example where the floor operations in (4) are actually needed, consider the lattice Λ with Gram matrix $\begin{bmatrix} 3 & 1 \\ 1 & 2 \end{bmatrix}$ and determinant 5 (this is the lattice 5_1 in the notation of [1]). Again there is no $v = (1, v_1, v_2) \in \mathbb{Z}^3$ such that Λ_v is geometrically similar to Λ. We take $L = \begin{bmatrix} \sqrt{3} & 0 \\ \frac{1}{\sqrt{3}} & \sqrt{\frac{5}{3}} \end{bmatrix}$, and find that

$$v = \left(1, \lfloor \sqrt{3}\, w \rfloor, \lfloor \sqrt{3}\, w \rfloor \lfloor \sqrt{5/3}\, w \rfloor + \lfloor w/\sqrt{3} \rfloor\right).$$

3.3. The lattice D_m, $m \geq 3$

As generator matrix for D_m^* we take ([3, p. 120])

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 1/2 & 1/2 & 1/2 & \dots & 1/2 & 1/2 \end{bmatrix} . \tag{7}$$

We set $w = 2t$, $t \in \mathbb{Z}$, and obtain

$$v = \left(1, 2t, (2t)^2, \dots, (2t)^{m-1}, t\frac{(2t)^m - 1}{2t-1}\right) .$$

In particular, when $m = 3$, we have

$$v = (1, 2t, 4t^2, 4t^3 + 2t^2 + t) , \tag{8}$$

for which Λ_v^* converges to the body-centered cubic lattice D_3^* and Λ_v to the face-centered cubic lattice D_3.

3.4. The lattice E_8

Using the generator matrix given in [3, p. 121], we find that $v = (1, v_1, v_2, \dots, v_8)$ is given by $v_1 = 2w$, $v_2 = 2w^2 - w$, $v_i = w(v_{i-1} - v_{i-2})$ for $i = 3, 4, \dots, 7$, and $v_8 = (w/2)(1 + \sum_{i=1}^{7} v_i)$, where w is even.

3.5. The Leech lattice

Using [3, Fig. 4.12], we find that $v = (1, v_1, v_2, \ldots, v_{24})$ is given by

$$\begin{aligned} v_1 &= 8w, \\ v_i &= 4w(v_{i-1}+1), \text{ for } i = 2, \ldots, 7, 9, 10, 11, 13, 17, \\ v_i &= 2w(\sum_{j \in S_i} v_j + 1), \text{ for } i = 8, 12, 14, 15, 16, 18, 19, 20, \\ v_i &= 2w \sum_{j \in S_i} v_j, \text{ for } i = 21, 22, 23, \\ v_{24} &= w(\sum_{i=1}^{23} v_i - 3), \end{aligned} \tag{9}$$

where $S_8 = \{1, 2, \ldots, 7\}$, $S_{12} = \{1, 2, 3, 8, 9, 10, 11\}$, $S_{14} = \{1, 4, 5, 8, 9, 12, 13\}$, $S_{15} = \{2k, 1 \le k \le 7\}$, $S_{16} = \{3, 4, 7, 8, 11, 12, 15\}$, $S_{18} = \{2, 4, 7, 8, 9, 16, 17\}$, $S_{19} = \{3, 4, 5, 8, 10, 16, 18\}$, $S_{20} = \{1, 4, 6, 8, 11, 16, 19\}$, $S_{21} = \{1, 2, 3, 4, 8, 12, 16, 20\}$, $S_{22} = \{8, 9, 12, 13, 16, 17, 20, 21\}$, $S_{23} = \{2k, k = 4, 5, \ldots, 11\}$.

4. Faster convergence

The construction in Theorem 2 produces a vector v of length $\|v\| = O(w^n)$, while from (6) we have $\|A - \frac{1}{w^2} A_v^*\|_\infty = O(\frac{1}{w}) = O(\frac{1}{\|v\|^{1/n}})$. It is sometimes possible to obtain a faster rate of convergence. Suppose Λ is D_3, and instead of (7) let us take the following generator matrix for D_3^*:

$$L := \begin{bmatrix} -1 & -1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Let

$$L_w = \begin{bmatrix} w-1 & w+1 & -w & 0 \\ -w-1 & w & -w+1 & 0 \\ -w & -w & -w & 1 \end{bmatrix} = \begin{bmatrix} -wL & \mathbf{0} \end{bmatrix} + \begin{bmatrix} \mathbf{0} & I_3 \end{bmatrix} + \begin{bmatrix} -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \tag{10}$$

with

$$A_v^* = L_w L_w^{\mathrm{tr}} = \begin{bmatrix} 3w^2+2 & w^2+1 & -w^2 \\ w^2+1 & 3w^2+2 & w^2 \\ -w^2 & w^2 & 3w^2+1 \end{bmatrix}. \tag{11}$$

The last matrix in (10) is chosen so that there are no terms of order w in (11). Let H_w denote the 3×3 matrix formed by the last three columns of L_w, and define v_1, v_2, v_3 by

$$H_w^{-1} L_w = \begin{bmatrix} -v_1 & 1 & 0 & 0 \\ -v_2 & 0 & 1 & 0 \\ -v_3 & 0 & 0 & 1 \end{bmatrix}.$$

Then

$$v = (1, v_1, v_2, v_3) = (1, 2w^2 - w + 1, 2w^2 + w + 1, 4w^3 + 3w) \tag{12}$$

has $\|v\| = O(w^3)$, and now $\|A - \frac{1}{w^2} A_v^*\|_\infty = O(\frac{1}{\|v\|^{2/3}})$, which is a faster convergence than we found in §3.3. We do not know if similar speedups are always possible. Incidentally, we first found (12)—before Theorem 1 was proved—by a combination of computer search and guesswork.

5. The fat strut problem

The problem studied in this paper arose when constructing codes for a certain analog communication channel [6]. The codes require that one finds a curved tube in the sphere S^{2n-1} which does not intersect itself, has a specified length and as large a volume as possible. The method used in [6] is based on finding a vector $v \in \mathbb{Z}^n$ with a specified value of $\|v\|$, such that there is a cylinder of large volume with axis $\overrightarrow{0v}$ which contains no points of $\mathbb{Z}^n$ other that 0 and v. The cross-section of the cylinder is an $(n-1)$-dimensional ball, and 0 and v are the centers of the two end-faces. The radius of the cylinder is taken to be as large as possible subject to the condition that the interior contains no point of $\mathbb{Z}^n$. The problem is to choose v, for a given length $\|v\|$, so that the volume of the resulting cylinder is maximized. We call a cylinder which achieves the maximal volume a *fat strut*.

A fat strut has the property that the projection of the cylinder onto $v^{\perp}$ does not contain the image of any nonzero point of $\mathbb{Z}^n$. The radius of the cylinder is therefore equal to the radius of the largest $(n-1)$-dimensional sphere in the projection lattice Λ_v which contains no nonzero point of Λ_v. In other words, finding a fat strut for a given length $\|v\|$ is equivalent to maximizing the density of the projection lattice Λ_v.

It is worth contrasting the fat strut problem with the result of [4] and [5] that for any lattice sphere packing in dimension three or higher there is always an *infinite* cylinder of nonzero radius (obviously not passing through the origin) which does not touch any of the spheres.

6. Acknowledgment

We thank the referee for some very helpful comments.

References

[1] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices I: Quadratic forms of small determinant, Proc. Royal Soc. London, **A 418** (1988), 17–41.

[2] J. H. Conway and N. J. A. Sloane, Low-dimensional lattices V: Integral coordinates for integral lattices, Proc. Royal Soc. London, **A 425** (1989), 211–232.

[3] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 3rd ed., 1998.

[4] A. Heppes, Ein satz über gitterförmige kugelpackungen, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*, **3–4** (1960/1961), 89–90.

[5] J. Horváth, Über die durchsichtigkeit gitterförmiger kugelpackungen, *Studia Sci. Math. Hungar.*, **5** (1970), 421–426.

[6] V. A. Vaishampayan and S. I. R. Costa, Curves on a sphere, shift-map dynamics, and error control for continuous alphabet sources, *IEEE Trans. Inform. Theory*, **49** (2003), 1658–1672.